



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/022,578	12/17/2001	Bhaskar Sinha	ONET-0101 PUS	6146
27256	7590	02/10/2006	EXAMINER	
ARTZ & ARTZ, P.C. 28333 TELEGRAPH RD. SUITE 250 SOUTHFIELD, MI 48034			POPHAM, JEFFREY D	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 02/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No. 10/022,578	Applicant(s) SINHA ET AL.	
	Examiner Jeffrey D. Popham	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 16 November 2005.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 December 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)             | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

***Remarks***

Claims 1-23 are pending.

***Response to Arguments***

1. Applicant's arguments filed 11/16/2005 have been fully considered but they are not persuasive.
2. The 35 U.S.C. 112, second paragraph rejections have not been overcome with the amendment. The claims are rejected under 35 U.S.C. 112, second paragraph, as being replete with errors including use of language that makes the claim scope and meaning unclear, inconsistencies within the claims, and antecedent basis problems that stem from incorrect dependencies, misspellings, etc. Claims 4, 7, 10, 11, and 13 still contain errors that make the claim scope and meaning unclear. Claims 1, 8, 22, and 23 still contain errors based on inconsistencies. Claims 1, 2, 3, 6, 9, 12, and 13 still contain errors based on antecedent basis.
3. Applicants argue that Grantges (U.S. Patent 6,324,648) does not disclose encrypting a ticket with a user password to form an encrypted ticket. The ticket is formed at the certificate authority and then sent back to the user computer via an SSL-encrypted session, wherein the session key for this SSL session is used as the user password.

4. Applicants argue that Wood (U.S. Patent 6,609,198) does not disclose forming a packet having a sequence number and a session key encrypted with the ticket. Wood discloses cryptographically securing session credentials, which include a sequence number (session ID; Column 9, lines 12-28) and that a session identifier can include a session key (Column 15, lines 3-8). Grantges also discloses that a session credential includes a session key (Column 8, lines 46-49). Wood discloses cryptographically securing the credentials, which, in the combination, will include at least a sequence number and session key. When a digital certificate is sent to the server, the user is authenticated, and the session credentials are encrypted with the password (SSL session's key) and sent back to the user's computer.

5. Page 9, paragraph 28 of applicant's specification states that tickets may include "various information such as lifetime indicator, a start time and an end time. The tickets may also include random numbers as part thereof to prevent duplication". It is unclear how to encrypt a packet with this ticket since the ticket does not contain any encryption keys, but at pages 10-11, paragraphs 32 and 33 there is a description of how to encrypt and decrypt with the ticket. Paragraph 32 does not disclose how exactly the encryption is performed, only that "Privilege server 26 validates the user and issues a sequence number and session key encrypted with the ticket to form a packet." Paragraph 33, however, discloses that decryption of the ticket is performed as follows: the client "decrypts the packet with the user password and provides the ticket and sequence number encrypted with the session key to the service desired such as data server 32."

This is the only description of how a packet is encrypted or decrypted "with the ticket". Since the password is a symmetric key used for both encryption and decryption as described in paragraph 31, this means that encrypting a packet with the ticket comprises encrypting the packet with the password. The combination of Grantges as modified by Wood does disclose encrypting a sequence number and a session key (as explained above) with the ticket by using this definition.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-23 are rejected under 35 U.S.C. 112, second paragraph, as they are replete with errors including use of language that makes the claim scope and meaning unclear, inconsistencies within the claims, and antecedent basis problems that stem from incorrect dependencies, misspellings, etc.

Examples are as follows:

- Claim 1, line 6 refers to "a head end server". This is inconsistent with the preamble, since the preamble already states that there is a head end server. For purposes of prior art rejection, it has been construed as "the head end server", so as to clearly claim that this is the same head end server claimed in the preamble. Claim 1, line 12 reads "forming a service access request token from the ticket and user identification". There is insufficient antecedent basis

- for this "user identification" in the claim. For purposes of prior art rejection, "user identification" has been construed as "user information".
- Claim 2, line 2 reads "negotiating the authentication scheme". There is insufficient antecedent basis for this limitation in the claims. For purposes of prior art rejection, it has been construed as "negotiating an authentication scheme".
  - Claim 3 contains the limitations "the server proxy" and "the user privilege proxy server". There is insufficient antecedent basis for these limitations in the claims. For purposes of prior art rejection, they have been construed as "the user privilege server proxy".
  - Claim 4 reads "A method as recited in claim 2 wherein the step of validating comprises validating the user in response to the user information in accordance with the authentication scheme." In claim 1, there are multiple recitations of validating, so it is unclear as to which one applicant intends for claim 4 to refer to. For purposes of prior art rejection, it has been construed as "A method as recited in claim 2 wherein the step of validating the user in response to the user information comprises validating the user with the authentication scheme."
  - Claim 6 recites the limitation "the encrypted ticket". There is insufficient antecedent basis for this limitation in the claims. For purposes of prior art rejection, claim 6 has been construed as being dependent upon claim 5.

- Claim 7, lines 2-3 read “forming a packet having a sequence number and session key encrypted with the ticket at the privilege server decrypting the packet at the user privilege server proxy.” This should apparently read “forming a packet having a sequence number and session key encrypted with the ticket at the privilege server and decrypting the packet at the user privilege server proxy.”
- Claim 12 contains the limitations “the web adapter”, “the service server”, “the session name”, “the user identification”, “the privilege server”, “the user”, and “the user ticket and privilege”. There is insufficient antecedent basis for these limitations in the claim. For purposes of prior art rejection, they have been construed as “a web adapter”, “a service server”, “a session name”, “a user identification”, “a privilege server”, “a user”, and “a user ticket and privilege”.
- Claim 13, lines 13-14 read “said privilege server generating a packet having a sequence number and a session key in response to the token”. The token is currently at the user privilege server proxy (just after generation), so it is unclear how the privilege server responds to a token that it has no idea has even been generated.

These are only examples, as there are many more errors in the claims, all of which must be corrected.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grantges (U.S. Patent 6,324,648) in view of Wood (U.S. Patent 6,609,198).

Regarding Claim 8,

Grantges discloses a method of authenticating a user having a user privilege server proxy (client computer/browser) for a network system having a privilege server (authorization server/certificate authority), a head end server (proxy server) and a web adapter (application gateway) comprising:

Negotiating an authentication scheme between the user privilege server proxy and privilege server (Column 4, lines 33-65);

Presenting user information to the web adapter (Column 12, line 57 to Column 13, line 17);

Presenting the user information to the head end server (Column 12, line 57 to Column 13, line 17);

Presenting the user information to the privilege server from the head end server (Column 12, line 57 to Column 13, line 17);



Validating the user at the privilege server in response to receiving the user information in accordance with the authentication scheme (Column 13, lines 8-41);

When the user is validated, generating a ticket for the user at the privilege server (Column 13, lines 8-41);

Encrypting the ticket with a user password to form an encrypted ticket (Column 7, line 63 to Column 8, line 14);

Providing the encrypted ticket to the user privilege server proxy through the head end server (Column 13, lines 18-41);

Decrypting the encrypted ticket (Column 7, line 63 to Column 8, line 14; and Column 13, lines 18-41);

Forming a service access request token from the ticket and user identification at the user privilege server proxy (Column 8, lines 16-28);

Sending the token from the user privilege server proxy to the privilege server (Column 8, line 29 to Column 9, line 18);

Validating the user in response to receiving the token (Column 9, lines 6-18);

Providing the packet to the head end server (Column 9, lines 6-18);

In response to receiving the packet, authenticating the user at the head end server (Column 9, lines 6-18; and Column 10, lines 6-25);

Providing the packet to the user privilege server proxy (Column 10, lines 6-25);

Sending the ticket and sequence number encrypted with the session key to a service server through the web adapter (Column 8, lines 40-51; and Column 11, line 63 to Column 12, line 10);

Validating the user at the service server (Column 11, lines 13-30);

Granting the user role based privileges at the service server (Column 11, line 63 to Column 12, line 10).

Grantges does not disclose forming a packet having a sequence number and session key encrypted with the ticket at the privilege server or decrypting this packet.

Wood, however, discloses validating the user in response to receiving the token (Column 12, line 52 to Column 13, line 10); forming a packet having a sequence number and session key encrypted with the ticket at the privilege server (Column 12, line 52 to Column 13, line 10); and decrypting the packet (Column 13, lines 27-44).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the credential level change system of Wood into the secure gateway of Grantges in order to allow credentials to be upgraded and downgraded as needed within the same session, so that a high security, overcredentialled log-on state is not required and need not be maintained (Column 2, lines 47-67).

Regarding Claim 1,

Claim 1 is a method claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 2,

Claim 2 is a method claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 4,

Claim 4 is a method claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 5,

Claim 5 is a method claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 6,

Claim 6 is a method claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 7,

Claim 7 is a method claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 13,

Claim 13 is a system claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 14,

Claim 14 is a system claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 22,

Claim 22 is a system claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 23,

Claim 23 is a method claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 9,

Grantges discloses that negotiating an authentication scheme between the user privilege server proxy and privilege server comprises presenting at least one security mechanism from the user privilege server proxy to the privilege server; and accepting or rejecting the at least one security mechanism at the privilege server (Column 4, lines 33-65).

Regarding Claim 3,

Claim 3 is a method claim that is broader than method claim 9 and is rejected for the same reasons.

Regarding Claim 10,

Grantges discloses that the step of validating at the privilege server is performed by a policy engine within the privilege server (Column 7, lines 29-44).

Regarding Claim 11,

Grantges discloses that generating a ticket comprises generating a ticket by encryption (Column 7, line 63 to Column 8, line 14).

Regarding Claim 12,

Claim 12 is a method claim that is broader than method claim 8, except for the steps of including a session name and choosing a service in the service server. Grantges discloses including a session name (Column 10, lines 32-53) and choosing a service in the service server (Column 9, lines 19-34).

Regarding Claim 15,

Grantges discloses that the user information comprises a user identification number (Column 14, lines 43-65).

Regarding Claim 16,

Grantges discloses that the privilege server has a policy engine therein (Column 7, lines 29-44).

Regarding Claim 17,

Grantges discloses that the privilege server comprises a key generator coupled to the policy engine (Column 12, line 52 to Column 13, line 10; and Column 15, lines 1-25).

Regarding Claim 18,

Grantges discloses that the privilege server comprises a proxy coordinator coupled to the policy engine (Column 9, lines 6-18).

Regarding Claim 19,

Grantges discloses that the privilege server comprises an obfuscator/deobfuscator coupled to the policy engine (Column 7, line 63 to Column 8, line 14).

Regarding Claim 20,

Grantges discloses that the privilege server comprise a store keeper coupled to the policy engine (Column 7, lines 29-44).

Regarding Claim 21,

Grantges discloses that the store keeper comprises a user information list (Column 7, lines 29-44).

Wood discloses that the store keeper comprises a user information list and a session information list (Column 12, line 52 to Column 13, line 10).

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2137

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
**EMMANUEL L. MOISE**  
**SUPERVISORY PATENT EXAMINER**